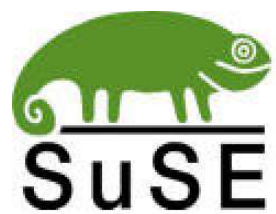


Machbarkeitsstudie

Konfiguration von Suse Linux 9.0





## **Inhaltsverzeichnis**

<b>Inhaltsverzeichnis.....</b>	<b>2</b>
<b>1. Vorbereitungen für die Serverkonfiguration.....</b>	<b>3</b>
<b>2. Konfiguration des DNS-Servers.....</b>	<b>3</b>
<b>2. Konfiguration des DHCP-Servers.....</b>	<b>8</b>
<b>3. Konfiguration eines Samba-Servers.....</b>	<b>11</b>
3.1 Was ist Samba? .....	11
3.2 Konfiguration von Samba.....	11
3.3 Einige wichtige Aspekte.....	12
Printers:.....	13
3.4 Einbinden der Clients in die Domäne.....	14
3.41 Beispielkonfiguration der smb.conf.....	16
<b>4. Automatisierung der Daemons.....</b>	<b>17</b>
<b>5. Zuweisen von Policies für einzelne Benutzer.....</b>	<b>18</b>
<b>6. Drucken unter Windows.....</b>	<b>19</b>
6.1 Linuxvorbereitung.....	19
6.2 Clienteinrichtung.....	23
<b>7. VNC-Server unter Suse Linux 9.0.....</b>	<b>24</b>
<b>8. Nvidia Grafikkartentreiber installieren.....</b>	<b>27</b>
<b>9. Installation eines NIS und NFS Servers.....</b>	<b>28</b>
9.1 Installation von NIS .....	28
9.2 Installation von NFS.....	29
<b>10. Konfiguration des Servers als Virens Scannerproxy...29</b>	
<b>11. Nachtrag.....</b>	<b>32</b>
<b>12. Quellenangaben.....</b>	<b>32</b>
<b>13. Verfasser.....</b>	<b>32</b>



## 1. Vorbereitungen für die Serverkonfiguration

Bevor mit der Konfiguration des Servers begonnen wird, sollte das Tool Webmin installiert werden. Unter Yast im Bereich Software hinzufügen oder entfernen nach Webmin suchen und auswählen. Nach der Yast-Installation muss das Tool allerdings noch konfiguriert werden. Dazu per Shell ins Verzeichnis `/usr/lib/webmin` wechseln und das Skript `setup.sh` mit dem Befehl `./setup.sh` aufrufen. Nach der Konfiguration steht einem Webmin mittels Browser über `localhost:10000` zur Verfügung. Die 10000 ist der Standardport für Webmin. Damit man von anderen Rechnern aus über Browser Zugriff auf Webmin und später Samba hat müssen im Ordner `/etc/xinetd.d` in den Konfigurationsdateien `Servers` und `Samba` im Bereich `only_from` die gewünschten IP-Adressen oder Subnetze eingestellt werden. Bei `disable no` eintragen. Unter Yast im Bereich `System-Runleveleditor xinetd` neu starten.

## 2. Konfiguration des DNS-Servers

Nun ist es an der Zeit den DNS-Server über Webmin zu konfigurieren. Als Benutzername und Passwort gibt man den des Root-Benutzers ein. Nun wechselt man über `Servers` auf `Bind DNS Server`. Unter `Existing DNS Zones` muss nun eine sogenannte `Forward -und Reverse-Lookup-Zone` erstellt werden. Die `Forward-Lookup-Zone` ist für die Auflösung `Name -> IP-Adresse` zuständig. Die `Reverse-Lookup-Zone` gerade für die umgekehrte Prozedur. Nun wird eine neue Zone über `create a new master zone` erstellt.



**Create Master Zone**

**New master zone options**

Zone type ☒ Forward (Names to Addresses) ☐ Reverse (Addresses to Names)

Domain name / Network

Records file ☒ Automatic ☐

Master server  ☒ Add NS record for master server?

Email address

Use zone template? ☐ Yes ☒ No

IP address for template records

Refresh time  seconds

Transfer retry time  seconds

Expiry time  seconds

Default time-to-live  seconds

Am Anfang wird ausgewählt welche der gerade angesprochenen Zonen man erstellen möchte. Wir fangen erst einmal mit der Forward an. Unter Domain name habe ich den viktiven namen saustall.local gewählt. Als Email address kann eine viktive ausgewählt werden. Wichtig ist, dass eine Adresse eingetragen wird, sonst klappt die Konfiguration nicht. Nach erfolgreicher Erstellung befindet man sich im Konfigurationsmenü:

**Edit Master Zone**

saustall.local

<b>A</b> Address (4)	<b>NS</b> Name Server (1)	<b>CN</b> Name Alias (0)	<b>MX</b> Mail Server (0)
<b>HI</b> Host Information (0)	<b>TX</b> Text (0)	<b>W]</b> Well Known Service (0)	<b>RP</b> Responsible Person (0)
<b>PT</b> Reverse Address (0)	<b>LO</b> Location (0)	<b>SR</b> Service Address (0)	<b>KE</b> Public Key (0)
<b>A MX NS PTR RR CN</b> All Record Types (5)			



Unter Address trägt man erst einmal den Namen und die IP-Adresse des Servers ein. Ganz wichtig ist, dass Update Reverse Yes (and replace existing) ausgewählt wird. Nach diesem Eintrag wechselt man wieder zum Anfangskonfigurationsmenü und erstellt eine Reverse-Lookup-Zone. Hier ist es wichtig bei Domain name / Network das Subnetz anzugeben. Wurden also für Server und Clients IP-Adressen der Art 192.168.100.x vergeben, muss man also 192.168.100 eintragen. Unter Reverse-Adresse wird nun automatisch die IP-Adresse eingetragen und es muss lediglich das letzte Oktett angepasst werden. Auch hier den Server eintragen und Update forward Yes wählen:

Reverse Address Records

In 192.168.100

Add Reverse Address Record

Address: 192.168.100. Time-To-Live: Default seconds

Hostname:

Update forward? ☒ Yes ☐ No

Create

Danach sind die Zonen erfolgreich konfiguriert worden und man kann Webmin, ohne starten des DNS-Servers verlassen.

### Existing DNS Zones

[Create a new master zone.](#) [Create a new slave zone.](#) [Create a new stub zone.](#) [Create a new forward zone.](#)

 <u>Root zone</u>	 <u>127.0.0</u>	 <u>192.168.100</u>	 <u>localhost</u>	 <u>saustall.local</u>
<a href="#">Create a new master zone.</a>	<a href="#">Create a new slave zone.</a>	<a href="#">Create a new stub zone.</a>	<a href="#">Create a new forward zone.</a>	

Der DNS-Server besteht unter Suse Linux aus mehreren Dateien in unterschiedlichen Verzeichnissen.

1. Named.conf im /etc - Verzeichnis.
2. Forward -und Reverse-Lookup-Dateien in /var/lib/named



In der `named.conf` muss nun Bind klar gemacht werden, dass er DDNS nutzen soll. Dazu müssen die selbsterstellten Zonen gesucht werden und die Zeile `allow-update { 192.168.100/24; }` eingetragen werden. Unten stehender Auszug aus meiner `named.conf` verdeutlicht dies nochmals:



```
options {  
  
    directory "/var/lib/named";  
    dump-file "/var/log/named_dump.db";  
    statistics-file "/var/log/named.stats";  
    auth-nxdomain yes;  
    forwarders { 192.168.100.254; };  
    listen-on port 53 { 192.168.100.1; };  
    listen-on-v6 { any; };  
    notify yes;  
    recursion yes;  
    interface-interval 5;  
    cleaning-interval 2;  
};  
  
zone "." in {  
    type hint;  
    file "root.hint";  
};  
  
zone "localhost" in {  
    type master;  
    file "localhost.zone";  
};  
  
zone "0.0.127.in-addr.arpa" in {  
    type master;  
    file "127.0.0.zone";  
};  
  
include "/etc/named.conf.include";  
  
zone "saustall.local" {  
    type master;  
    file "saustall.local";  
    allow-update { 192.168.100/24; };  
    notify yes;  
};  
  
zone "100.168.192.in-addr.arpa" {  
    type master;  
    file "192.168.100.rev";  
    allow-update { 192.168.100/24; };  
    notify yes;  
};
```



Nun werde ich einzelne Bereiche der Named.conf erläutern, die für eine eigene Konfiguration von Belang sind:

1. 

```
forwarders { 192.168.100.254; };
```

Hier werden sogenannte Router eingegeben. Sprich, falls der Linux DNS-Server die Anforderungen der Clients nicht beantworten kann, werden diese an den sogenannten Standard-Gateway weitergeleitet. Erst wenn dieser ebenfalls nichts damit anfangen kann, kommt eine Fehlermeldung.

2. 

```
listen-on port 53 { 192.168.100.1; };
```

Hier wird ein Port für unseren DNS-Server definiert. Dieser dient etwa den NSLOOKUP-Anfragen der Clients.

## 2. Konfiguration des DHCP-Servers

Jetzt geht es an das Einrichten des DHCP-Servers. Dieser wird über Yast direkt eingerichtet. Auch hier könnte man den DNS-Server mittels Webmin konfigurieren, allerdings hatte dies nie recht bei mir funktioniert. Um den DHCP-Server zu konfigurieren wechselt man unter Netzwerkdienste DHCP-Server. Als erstes aktiviert man den automatischen Start des Servers beim Booten. Danach wird ein neues Subnetz erstellt. In unserem Fall die 192.168.100.0 255.255.255.0. Nun muss dieses Subnetz noch konfiguriert werden. Der folgende Screenshot zeigt die in unserem Beispiel wichtigen Einstellungen:





### Konfiguration des Subnetzes

Option	Wert
subnet	192.168.100.0
netmask	255.255.255.0
-----	
option domain-name	"saustall.local"
option domain-name-servers	192.168.100.1
option routers	192.168.100.254
range	192.168.100.4 192.168.100.253

Danach geht es an den Anfang der Konfigurationseinstellungen. Diese sollten wie folgt angepasst werden:

### Konfiguration des DHCP-Servers

Option	Wert
DHCP-Server beim Systemstart aktivieren	Ja
Firewall anpassen	Ja
Subnetze	
Hosts	
Netzwerkschnittstellen	eth0
-----	
authoritative	
ddns-update-style	interim
ddns-updates	on
default-lease-time	600
log-facility	local7
max-lease-time	7200

Danach auf Beenden klicken, um die Einstellungen zu speichern. Unter /etc/dhcpd.conf sollten nun folgende Einträge stehen:



```
#
# This file was generated by YaST2.
#
# If you update it manually, YaST2 component for DHCP server
# configuration will rewrite it next time you use it.
#
# Creation time: Sun Sep 12 10:41:51 CEST 2004
#

authoritative ;
ddns-update-style interim;
ddns-updates on;
default-lease-time 600;
log-facility local7;
max-lease-time 7200;

subnet 192.168.100.0 netmask 255.255.255.0 {
    option domain-name "saustall.local";
    option domain-name-servers 192.168.100.1;
    option routers 192.168.100.254;
    range 192.168.100.4 192.168.100.253;
}
```

Wenn die Konfiguration der Serverdienste abgeschlossen ist, kann nun mit der Konfiguration zweier Dateien in /etc begonnen werden. Host.conf, nsswitch.conf. In Host.conf muss ein Eintrag namens „order bind, hosts“ hinzugefügt werden. Damit werden bei dynamischen Aktualisierungen die DNS-Einträge direkt bevorzugt. In der Datei nsswitch.conf müssen folgende Einträge folgendermaßen umgeändert werden: „hosts: dns files“ und „networks: dns files“. Hier wird nun auch DNS bevorzugt.

Ganz wichtig ist es nun die Besitzerrechte von /var/lib/named von root auf named unter Benutzer und Gruppe, incl. das Häkchen für die Übernahme der untergeordneten Ordner und Dateien gleich mit anklicken, abzuändern. Sonst ist es named nicht möglich sogenannte Journal-Dateien für die Forward -und Reverselookup-Zonen zu erstellen. Folgedessen kann auch die Dynamische Aktualisierung nicht funktionieren.



## 3. Konfiguration eines Samba-Servers

### 3.1 Was ist Samba?

Samba ist ein Programmpaket, das (z.B. Windows-) Clients erlaubt komfortabel auf Datei- und Druckressourcen eines Unixservers zuzugreifen. Dafür implementiert Samba das SMB-Protokoll (Server Message Block), das in Windows bzw. LAN Manager Netzwerken verwendet wird, um Ressourcen anzubieten. Der Unixrechner sieht mit Samba in einem solchen Netzwerk wie ein NT Server aus. Er erscheint in der Netzwerkumgebung von Windows-Clients und exportiert Verzeichnisse und Drucker.

Die jeweils aktuellste Version ist unter [samba.anu.edu.au](http://samba.anu.edu.au) erhältlich.

Da nun DNS und DHCP eingerichtet wurden, kann man sich nun um die Konfiguration des Samba-Servers als File -und Printserver incl. Domänenkontroller kümmern.

### 3.2 Konfiguration von Samba

Für die Sambakonfiguration gibt es ein grafisches Tool namens Swat. Es ermöglicht die Konfiguration von Samba mittels Browseroberfläche.

Um diesen Service nutzen zu können, muss Swat erst freigeschaltet werden. Dazu muss in das Verzeichnis `/etc/xinetd.d/samba` gewechselt werden. Im Bereich `only_from` muss die Netzwerkadresse (hier: `192.168.100.0/24`) angegeben werden und bei `disable = yes` auf `no` setzen. Danach ist Swat freigeschaltet. Danach wird wieder `xinetd.d` in Yast mittels Runleveleditor neu gestartet. Nmb und smb bekommen die Runlevel 3 und 5 und werden aktiviert. Im Browser gelangt man über <http://IP-Adresse:901> ins Konfigurationsmenü.



### 3.3 Einige wichtige Aspekte

#### Globals:

- Angabe, ob der Server als Domänencontroller fungieren soll.
- Angabe von Anmeldescripte
- Angabe der Gruppe der Domänenadministratoren
- Um den Windows-Clients den Zugang zum Samba-Server zu ermöglichen sollte im Bereich Logon-Option unter add user script /usr/sbin/useradd -d/dev/null -g 100 -s /bin/false -M %u stehen. Somit werden beim Domänenbeitritt die Maschinenkonten automatisch, sprich „On the Fly“ übertragen und konfiguriert. Unter der Rubrik logon script kann Beispielsweise [\\server\netlogon\%u](#) stehen. Wenn sich nun ein User anmeldet, sucht Samba im Verzeichnis Netlogon nach einer Batchdatei, die genau gleich lautet wie der Anmeldename des Benutzers. Somit können für verschiedene User unterschiedliche Laufwerke gemappt werden.

#### Shares:

- Erstellen von Verzeichnissen, die gemappt werden sollen
- Rechteverwaltung der Administratoren und Benutzer auf die Shares
- Wichtig: Da ich im Global-Bereich ein Netlogon-Verzeichnis für die Scriptverteilung angegeben habe, muss dies natürlich erst erstellt und dann mittels dem Shared freigegeben werden. Man sollte sich also direkt auf dem Server eine sinnvolle Strukturierung seiner Verzeichnis -und Datenbestände machen.



### Printers:

- Wie es der Name schon vermuten lässt, können hier die Drucker, die direkt am Server Angeschlossen sind, für die Windows-Clients freigegeben werden. Für den weiteren Betrieb sind eigentlich keine weiteren Punkte in dieser Rubrik von Wichtigkeit.

### Wizard:

- Im Wizard kann man nochmals allgemeine Konfigurationen zum Server angeben, sprich der Domainname, Netbiosname, ob er überhaupt als Domaincontroller fungieren soll, etc.

### Status:

- Im Status-Bereich kann der Samba -und Netbios-Dienst gestartet oder restarted werden.
- Ganz wichtig: Werden im Globals und -Wizard-Bereich Änderungen vorgenommen, müssen die beiden Dienste restarted werden.

### View:

- Im View-Bereich kann man sich die sogenannte smb.conf einsehen. In dieser Konfigurationsdatei, die sich unter /etc/samba/smb.conf verbirgt, werden alle Einstellungen gespeichert, die unter SWAT vorgenommen wurden.

### Password:

- Unter Password müssen nun alle am Server angelegten Benutzer, die auf Samba zugreifen sollen angelegt und aktiviert werden. Nun muss also



unter Samba im Password-Bereich der User root incl. Passwort eingetragen, sprich created werden, anschließend enabled werden. Erst dann kann man sich mit dem Benutzer über einen Windows-Client am Server, sprich also in der Domäne anmelden.

### Allgemein:

- Viele Bereiche sind eigentlich selbsterklärend, weshalb ich hier nicht näher darauf eingehen werde. Am Ende füge ich noch eine Beispielskonfiguration der smb.conf an.

## **3.4 Einbinden der Clients in die Domäne**

### Windows XP:

Als erstes muss unter Windows XP im Registry-Editor nach dem Schlüssel requiresignorseal gesucht werden und den Eintrag auf 0 abändern. Sonst kann man sich trotz erfolgreichem Domänenbeitritt nicht an der Domäne einloggen, da die Fehlermeldung kommt, dass entweder die Domäne nicht vorhanden ist, oder der Benutzername oder das Kennwort ungültig sind. Unter Windows XP kann man folgendermaßen der Domäne beitreten:

Rechte Maustaste auf Arbeitsplatz-Eigenschaften-Computernamen-Ändern. Hier sollte ein sinnvoller Rechnername beispielsweise WS1, wie in unserer Machbarkeitsstudie auch verwendet, genommen werden. Im Bereich Weitere wird in unserem Fall das DNS-Suffix saustall.local eingetragen. Unter Domäne ebenfalls saustall.local. Es erfolgt nach einer kurzen Zeit eine Eingabemaske, in der root und das Passwort eingetragen werden müssen, da nur root die Rechte hat, Clients in die Domäne mit aufzunehmen. Nach einer kurzen Zeit sollte „Willkommen in der Domäne saustall.local“ erscheinen und der Rechner fordert zum Neustart auf. Nach dem Neustart sollte man sich nochmals lokal anmelden und wieder in den Bereich Computernamen wechseln. Nun über Netzwerkerkennung nochmals derselben Domäne beitreten. Dies ist wichtig, da man nun die Möglichkeit hat, den Benutzer Root direkt als Administrator für den Client hinzuzufügen.



**Erscheinungsbild nach erfolgreicher Anwendung**



### 3.41 Beispielkonfiguration der smb.conf

```
# Samba config file created using SWAT
# from ws1.saustall.local (192.168.100.2)
# Date: 2004/09/23 21:27:42

# Global parameters
[global]
    workgroup = SAUSTALL.LOCAL
    netbios name = SERVER
    encrypt passwords = Yes
    map to guest = Bad User
    admin log = Yes
    time server = Yes
    unix extensions = Yes
    socket options = SO_KEEPALIVE IPTOS_LOWDELAY TCP_NODELAY
    printcap name = CUPS
    add user script = /usr/sbin/useradd -d /dev/null -g 100 -s /bin/false -M %u
    logon script = \\server\sharedfiles\netlogon\%u
    logon path =
    logon home =
    domain logons = Yes
    os level = 2
    winbind use default domain = Yes
    admin users = root
    printer admin = root
    hosts allow = 192.168.100.
    printing = cups
    veto files = /*.eml/*.*.nws/riched20.dll/*.*{*/
```





```
[printers]
comment = All Printers
path = /var/tmp
create mask = 0600
printable = Yes
browseable = No

[print$]
comment = Printer Drivers
path = /var/lib/samba/drivers
write list = @ntadmin root
force group = ntadmin
create mask = 0664
directory mask = 0775

[sharedfiles]
path = /sharedfiles
write list = mroth
read only = No

[netlogon]
path = /sharedfiles/netlogon
read only = No

[benutzerdaten]
path = /benutzerdaten
read only = No
```

## 4. Automatisierung der Daemons

Unter Linux werden die Dienste als Daemons bezeichnet. Da ja der DNS - DHCP und Samba-Server auch nach Neustarts verfügbar sein sollen, müssen im Yast-Kontrollzentrum unter System-Run-Level-Editor die Dienste nmbd (Netbios), smb (Samba), dhcp (DHCP-Server), named (DNS-Server (Bind9)) und xinetd (Swat-Einstellungsconsole) auf Runlevel 3 und 5 gestellt werden.

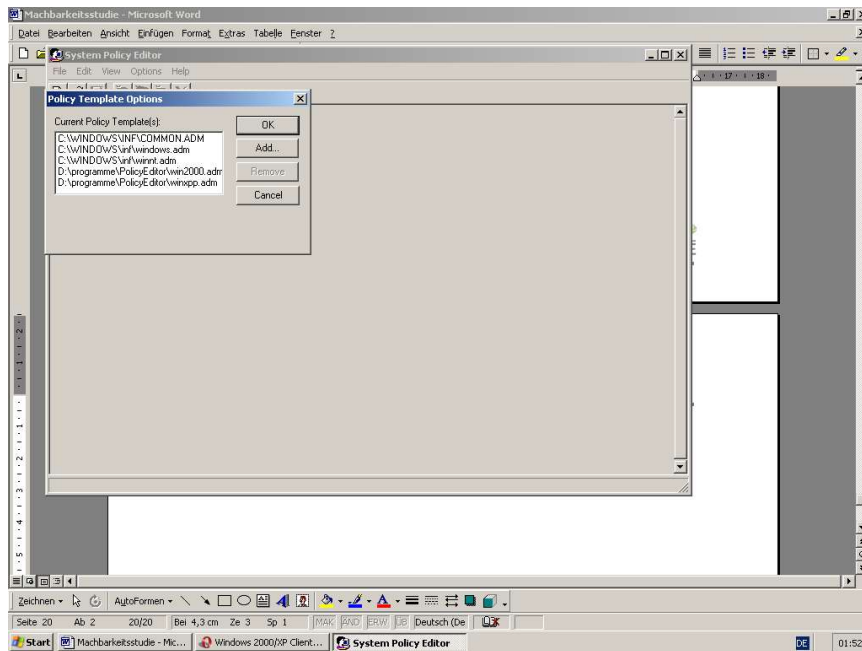


## 5. Zuweisen von Policies für einzelne Benutzer

Unter Linux kann man leider nicht direkt Rechtevergabe auf einzelne Computer, Gruppen oder Benutzer tätigen. Durch einen kleinen Trick jedoch geht es trotzdem. Es muss ein sogenanntes Programm namens Poledit auf einem beliebigen Windows-Client installiert werden. Im Internet gibt es dazu verschiedene ADM-Dateien für verschiedene Microsoft-Betriebssysteme. Wurden diese eingebunden kann man mittels Poledit Computer -und Benutzereinstellungen tätigen, um den User in seiner Handlungsfähigkeit einschränken zu können. Bei Windows XP muss zusätzlich der Registryeditor herangezogen werden, um die Pfadangabe zur Pol-Datei anzugeben. Bei Windows 2000 war dies nicht nötig. Folgender Pfad muss editiert werden.

HKEY\_LOCAL\_MACHINE\ System\ CurrentControlSet\ Control\ Update.  
Erstellen Sie einen Wert mit dem Namen "NetworkPath" als Datentyp REG\_SZ und geben Sie hier den Pfad zur Policy-Datei an (z.B.: "\\<Servername>\<Freigabename>\<Name>.POL").

Die Policy Datei kann dann direkt im Netlogon-Verzeichnis abgespeichert werden. Somit „verteilt“ auch Linux Rechte.



**Policy-Editor. Auswahl der ADM-Dateien für verschiedene Betriebssysteme.**

## 6. Drucken unter Windows

### 6.1 Linuxvorbereitung

Im Verzeichnis `/etc/cups/` gibt es eine Datei namens `cupsd.conf`. In dieser Datei kann man Einstellungen vornehmen, um eine Druckerkonfiguration bequem über Webbrowser am Server, als auch an Clients vornehmen zu können. Dazu sind folgende Schritte notwendig:

Suchen Sie jetzt nach folgenden Einstellungen und ändern diese dementsprechend ab.

```
# PreserveJobHistory Yes
```

```
# PreserveJobFiles No
```



Sollen ihre fertigen, gestoppten und abgebrochenen Druckaufträge gelöscht werden, entfernen Sie bei beiden Zeilen das # am Anfang und setzen Sie auf No.

```
# AutoPurgeJobs No
```

Diese Option sollten sie auf Yes setzen und das # entfernen.

Danach folgende Einträge suchen:

```
<Location />  
Order Deny,Allow  
Deny From All  
Allow From 127.0.0.1  
Allow From 127.0.0.2  
</Location>
```

Fügen Sie nach den beiden "Allow From" Zeilen die folgende Zeile ein:

```
Allow From 192.168.100.0/24
```

Am Ende dieses Abschnittes sollten Sie ebenfalls die obige Zeile anfügen.

```
## Restrict access to local domain  
Order Deny,Allow  
Deny From All  
Allow From 127.0.0.1
```

Nachdem Sie die cupsd.conf angepasst haben, starten die den Cups-Dämon und aktivieren ihn im Runlevel Editor:

cups und wieder die Runlevels auf 3 und 5 setzen.

Jetzt können Sie von einem Client unter der folgenden Webadresse ihren Drucker einrichten:

<http://192.168.100.1:631>



Nach einem Klick auf Administration erscheint eine Passwortabfrage, tragen Sie den Benutzer root ein und dessen Passwort. Danach klicken Sie auf "Add Printer" geben den Druckernamen, den Druckerport (LPT1 = /dev/lp0) und eine Druckerbeschreibung ein. Auf der nächsten Seite wählen Sie den Druckerport aus, in diesem Beispiel ist dies "Parallel Port #1". Nun müssen Sie den Hersteller und den Druckertyp auswählen. Nachdem Sie den Drucker eingerichtet haben, wechseln Sie zu "Printers" und testen die Druckerkonfiguration indem Sie auf "Print Test Page" klicken. Wenn ihre Druckerkonfiguration in Ordnung ist, müssen Sie nur noch den Drucker über Samba freigeben. Dazu können Sie entweder SWAT verwenden oder die smb.conf manuell anpassen. Folgenden Abschnitt sollten Sie am Ende der smb.conf einfügen:

```
[Printer1]
```

Dies ist der Freigabenamen und sollte aussagekräftig sein.

```
comment = Epson Stylos Color 740
```

Der Kommentar ist optional.

```
path = /tmp  
hosts allow = 192.168.100.
```

Hier können Sie angeben welche Netzwerke bzw. Rechner drucken dürfen. In diesem Beispiel sollen alle Clients mit der IP-Adresse 192.168.100.x drucken dürfen.

```
printable = Yes
```

Muss auf Yes gestellt sein damit man drucken kann.

```
printer name = printer1
```

Tragen Sie hier den Druckernamen den Sie bei cups eingestellt haben ein.

```
printer driver = Epson Stylos Color 740
```

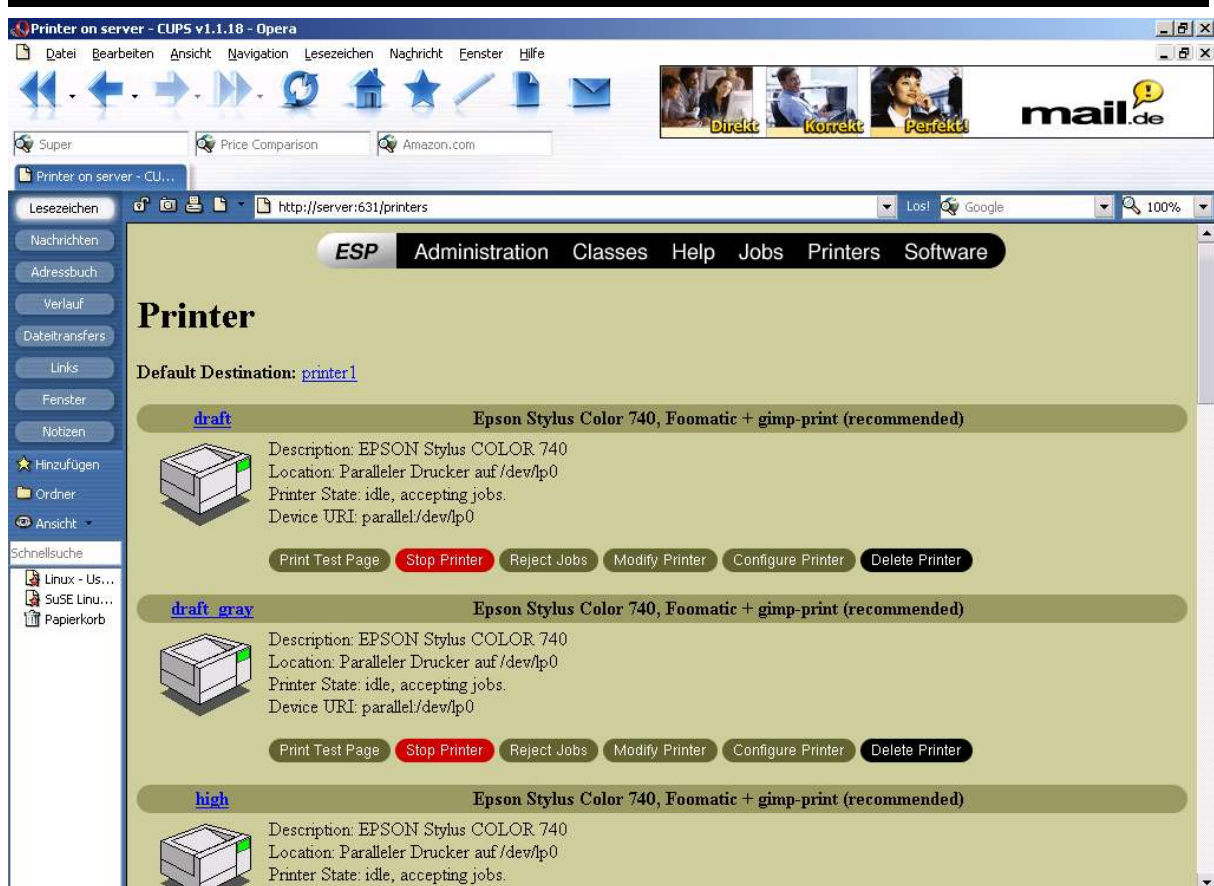


Hier sollten Sie den Druckertreiber eintragen, bei Windows 2000 und XP Clients wird dann nicht nach einem Druckertreiber gefragt.

Nachdem Sie die smb.conf angepasst haben, starten Sie Samba neu.

`rcsmb restart`

Nun können Sie den Drucker auf ihrem Client einrichten und danach verwenden.



Nach erfolgreicher Konfiguration sieht man dieses Bild

### 6.2 Clienteinrichtung

Um nun unter Windows auf einen Drucker zugreifen zu können, der an dem Samba-Server hängt, ist ein sogenannter Postscript-Treiber notwendig. Diesen gibt es auf der Adobe-Homepage ([www.adobe.com](http://www.adobe.com)) zum download. Falls man mehr mit seinem Drucker machen oder einstellen möchte, dann sind noch zusätzlich sogenannte ppd-Dateien wichtig. Diese geben beispielsweise den Zugriff auf unterschiedliche Papierschächte frei. Diese Dateien können ebenfalls bei Adobe heruntergeladen, oder per Google bezogen werden. Der Postscript-Treiber wird nun per Doppelklick installiert. Als Druckerort wählt man in diesem Fall Netzwerkdrucker aus und sucht danach über das Netzwerk den gewünschten Drucker aus. Danach geht es an die ppd-Datei. Standardmäßig liefert der Adobe Postscript-Treiber eine Standard-ppd-datei mit. Falls man von der Adobe-Homepage eine ppd-Datei heruntergeladen hat, kann man dann auch



diese angeben. Danach wird der Postscripttreiber inclusive der ppd-Datei installiert und dem Drucken steht nichts mehr im Wege.

## 7. VNC-Server unter Suse Linux 9.0

Um VNC unter Linux nutzen zu können, müssen Sie unter /etc/xinetd.d die Datei vnc aufsuchen. Dort kann man nun für verschiedene Ports VNC freischalten, indem man disable=yes auf no setzt. Aktiviert man beispielsweise vnc10 kann man nach anschließendem Neustart der Xinetd.d im Runleveleditor über einen Client mit VNC-Anbindung mit dem Befehl <IP-Adresse>:10 auf den VNC-Server zugreifen.

(Bei Suse Linux 9.0 genügt bereits beispielsweise bei der Installation die Bestätigung der Vernwartung dieses Rechners. Somit müssen obig genannte Änderungen nicht vorgenommen werden.)





```
# default: off
# description: This serves out a VNC connection which starts at a KDM login \
#      prompt. This VNC connection has a resolution of 1024x768, 16bit depth.
service vnc10
{
    socket_type    = stream
    protocol       = tcp
    wait           = no
    user           = nobody
    server         = /usr/X11R6/bin/Xvnc
    server_args    = :42 -inetd -once -query localhost -geometry 1024x768 -depth
                     16
    type           = UNLISTED
    port           = 5910
}
# default: off
# description: This serves out a VNC connection which starts at a KDM login \
#      prompt. This VNC connection has a resolution of 1280x1024, 16bit depth.
service vnc11
{
    type           = UNLISTED
    port           = 5911
    socket_type    = stream
    protocol       = tcp
    wait           = no
    user           = nobody
    server         = /usr/X11R6/bin/Xvnc
    server_args    = :42 -inetd -once -query localhost -geometry 1024x768 -depth 16
    disable        = yes
}
# default: off
# description: This serves out the vncviewer Java applet for the VNC \
#      server running on port 5910, (vnc port 10).
```



```
service vnchttpd10
{
    socket_type    = stream
    protocol       = tcp
    wait           = no
    user           = nobody
    server         = /usr/X11R6/bin/vnc_inetd_httpd
    server_args    = 1024 768 5910
    type           = UNLISTED
    port           = 5810
}
# default: off
# description: This serves out the vncviewer Java applet for the VNC \
#              server running on port 5911, (vnc port 11).
service vnchttpd11
{
    type           = UNLISTED
    port           = 5811
    socket_type    = stream
    protocol       = tcp
    wait           = no
    user           = nobody
    server         = /usr/X11R6/bin/vnc_inetd_httpd
    server_args    = 1280 1024 5911
    disable        = yes
}
```



## 8. Nvidia Grafikkartentreiber installieren

Als Erstes sollte man sich vergewissern, ob die sogenannten Kernel-Header-Files installiert sind. Diese können gegebenenfalls im Yast-Kontrollzentrum unter Kernel-Entwicklung -> evlog-devel nachgeholt werden. Am Besten man installiert die kompletten C/ C++ Compiler und Werkzeuge und die Kernel Entwicklung. Nun kann man unter [www.nvidia.com](http://www.nvidia.com) unter linux IA32 eine sogenannte Run-Datei herunterladen. Diese sollte in einem geeigneten Verzeichnis abgelegt werden. Da die Installation des Grafikkartentreibers nur in der reinen Konsole stattfinden kann, empfiehlt es sich ab jetzt unter Yast im Runleveleditor bei dem X Display Manager (xdm) den Runlevel 5 zu deaktivieren und dies abzuspeichern. Nach einem Neustart kann man sich nun direkt unter der Konsole anmelden. Nun sollte man in das Installationsverzeichnis wechseln und die Datei entpacken. Dazu wird folgender Befehl verwendet `sh *.run --extract-only cd / <installationsverzeichnis>`. Nun wird ein Verzeichnis innerhalb des Installationsordners mit dem gleichen Namen wie die Run-Datei gebildet. Wechselt man in dieses Verzeichnis, so findet man eine ausführbare Datei namens nvidia-installer vor. Dies startet man mit folgendem Befehl `./nvidia-installer`. Danach wird der Grafikkartentreiber installiert. Achtet bitte darauf, dass eine funktionstüchtige Internetverbindung während der Installation besteht, da das Installationsprogramm nach bereits vorkompilierten Kernels ausschau halten möchte. Leider habe ich bis jetzt nur Erfahrung mit einem Default-Router zur Internetverbindung gemacht, weshalb ich bei eventuellen Fragen auch nur darauf eingehen kann. Mit dem Befehl `xinit` gelangt man von der Konsole, der sogenannten Shell, wieder in seine grafische Oberfläche. Im Runleveleditor sollte man nun den Runlevel 5 wieder aktivieren, damit die GUI automatisch mit Linux startet.

Merke:

Alternativ kann der Grafikkartentreiber auch mit dem Befehl `sh *.run -q` temporär entpackt und installiert werden.



## 9. Installation eines NIS und NFS Servers

Hat man Linux-Clients im Netzwerk möchte man auch mit diesen in den Genuss einer einheitlichen Benutzerverwaltung kommen und einfachen Zugriff auf etwaige Fileserver haben. Hier kommt NIS und NFS ins Spiel. Mittels NIS werden auf dem Server unter Yast-Sicherheit und Benutzer-Benutzer bearbeiten und anlegen die gewünschten User und Gruppen angelegt und den Clients zur Verfügung gestellt, also wie etwa bei einem Samba-Server. Mit NFS werden einzelne Verzeichnisse auf dem Server freigegeben, die dann auf dem Client gemountet werden können.

### 9.1 Installation von NIS

Um NIS einrichten zu können, wechselt man unter Yast auf Netzwerkdienste NIS-Server. Als nächstes wählt man NIS Master Server neu konfigurieren. Als NIS Domainname sollte man den gleichen wie unter Samba verwenden, hier also saustall.local. Zudem sollte noch die schnelle Map-Verteilung (rpc.ypxfrd) ausgewählt werden. Danach zweimal auf Weiter klicken und bei der Host-Konfiguration beispielsweise das gewünschte Subnetz hinzufügen. Hier also wieder 192.168.100.0 255.255.255.0. Danach auf beenden klicken und der NIS-Server wird vollends von Linux selbst konfiguriert. Am NIS-Client wechselt man unter Yast-Netzwerkdienste-Nis-Client. Natürlich soll NIS gestartet werden. Hier kann auch gleich ein Automounter aktiviert werden, der automatisch Dateien und Verzeichnisse mounten kann. Als NIS-Domain wählt man hier saustall.local und als Adressen der NIS-Server die IP-Adresse des gewünschten NIS-Servers. Mit einem Klick auf beenden wird der Client fertig konfiguriert.



## 9.2 Installation von NFS

Um NFS einrichten zu können, wechselt man unter Yast auf Netzwerkdienste NFS-Server. Als erstes NFS-Server starten, danach kann man die gewünschten Verzeichnisse hinzufügen. Als Zugriffsberechtigte kann man etwa alle Rechner der Domäne saustall.local eintragen. Dazu wählt man unter Rechner (Wildcard) \*.saustall.local und für Optionen rw,no\_root\_squash,sync. Mit einem Klick auf beenden ist der NFS-Server eingerichtet. Am NFS-Client wechselt man unter Yast-Netzwerkdienste-NFS-Client. Auf Hinzufügen klicken und den gewünschten NFS-Server und Verzeichnisse auswählen. Wichtig ist hier, wo die einzelnen Verzeichnisse auf dem Server gemountet werden sollen. Möchte man das Homeverzeichnis der User auf dem Server freigeben, da wir ja ebenfalls NIS konfiguriert haben, kann man dies auf dem Client direkt unter /home mounten. Somit hat man sich leicht servergespeicherte Profile angelegt.

## 10. Konfiguration des Servers als Virens Scannerproxy

Eine interessante Sache, bezüglich der Sicherheitskonfiguration eines Linux-Netzwerkes ist Squid. Squid ist ein Proxyserver für Linux. Mit Hilfe des Programmes Surfprotect kann man seinen Proxyserver so konfigurieren, dass dieser automatisch Dateien nach Viren durchsucht, die ein Client herunterladen möchte. Dieses Beispiel soll mit dem Virens Scanner Antivir erklärt werden. Andere Virens Scanner wie Sophos oder Clamav sind ebenfalls möglich. Ich habe mir hier die Workstationversion von Antivir heruntergeladen. Diese ist ebenfalls für private Zwecke kostenlos. Nach der Registrierung bekommt man eine Schlüsseldatei. Somit kann man für ein Jahr Updates beziehen. Als erstes müssen Squid, Squidguard und ein Apache-Server mit PHP installiert werden. Unter Suse geschieht dies unter Yast-Software installieren oder löschen. Für den Apache mit PHP sollte man einfachheitshalber die ganze Rubrik einfacher Webserver komplett installieren. Squidguard ist zur Rechtekonfiguration gedacht. Über dieses Plugin wird später Surfprotect mit Virens Scanner beim Download bestimmter Dateien, wie beispielsweise .exe,.bat, etc. aufgerufen. Nach der Installation der Programme muss Squid mit Squidguard bekannt gemacht werden. Dazu muss die Datei /etc/squid/squid.conf editiert werden. In Zeile 985 muss der Eintrag „**redirect\_program /usr/sbin/squidGuard**“ hinzugefügt werden. In Zeile 1760 wird die Zugriffssteuerung für einzelne



Clients oder ganze Subnetze geregelt. Folgender Eintrag berechtigt unser gesamtes Subnetz 192.168.100.0/24 den Zugriff auf den Proxyserver:

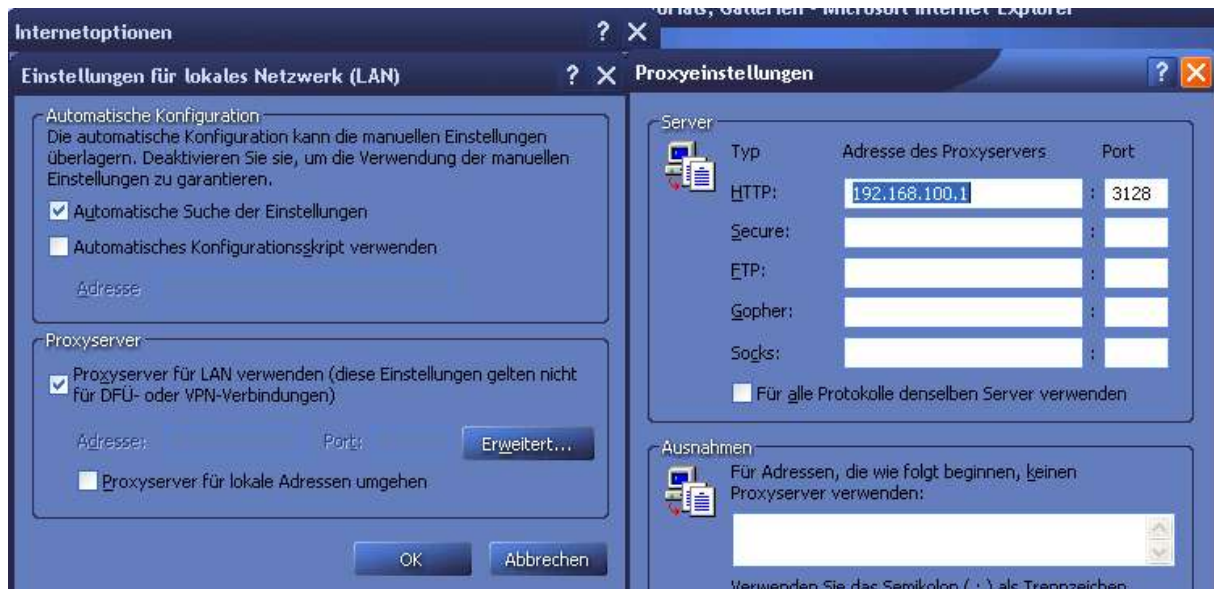
```
„acl our_networks src 192.168.100.0/24  
http_access allow our_networks  
http_access deny all“
```

Nach dieser Konfiguration kann Surfprotect eingerichtet werden. Dieses kann man unter <http://surfprotect.sf.net> herunterladen. Nun wird das Verzeichnis Surfprotect in /srv/www/htdocs eingerichtet und das heruntergeladene Archiv in dieses entpackt. Als nächstes werden die Cacheverzeichnisse für Surfprotect eingerichtet. Unter /var/cache muss das Verzeichnis surfprot angelegt werden. Mit der rechten Maustaste draufklicken und unter Berechtigung als Eigentümer wwwrun und als Gruppe www eintragen. Der Eigentümer und die Gruppe sollen alle Berechtigungen bekommen. Ebenso ist unter der Gruppe das GID zu setzen. Nun legt man unter /var/tmp das Verzeichnis surfprot\_quarantine an und die Rechtevergabe wie oben bereits geschildert setzen. Unter /srv/www/htdocs/surfprotect befindet sich eine Datei namens squidguard.conf diese enthält eine Zeile beginnt mit (.\*%surfprotect\_enter%\$|\ .... Diese Zeile muss in eine Datei, die wir zuerst noch erstellen müssen. Diese Datei namens criticalsuffixes ist unter /var/lib/squidGuard/db/blacklist zu erstellen. Der Rest des Inhalts aus squidguard.conf ist in der gleichnamigen Datei unter /etc abzuspeichern. Der bereits vordefinierte Inhalt der Datei /etc/squidGuard.conf kann gelöscht werden. Aber vorsichtshalber eine Sicherungskopie dieser Konfigurationsdatei anfertigen. Nun sollte man unter /srv/www/htdocs/surfprotect/surfprot.defaults den Eintrag define (SCANNER\_INCLUDE, „surprot\_hbav.inc“); aktivieren und das bereits aktivierte Fakescannmodul von Surfprotect deaktivieren. Diese Einträge finden sich normalerweise ganz unten in der Datei. Danach kann unter [www.antivir.de](http://www.antivir.de) die Linux-Workstation-Version heruntergeladen und registriert werden. Nach der Installation und der Registrierung dieses Produktes sollte man den per e-mail erhaltenen Lizenzschlüssel nach /usr/lib/AntiVir/ kopieren. Dies muss unbedingt vor dem ersten Start von Antivir erfolgen. Ebenfalls sehr interessant ist die Datei surfprot\_hbav.inc. Hier kann man beispielsweise noch einstellen, ob Antivir auch Spiele oder andere Software durchsuchen soll. Nach diesen ganzen Vorbereitungen kann nun unter Yast-System-Runleveleditor der Apache und squid gestartet werden. Am besten

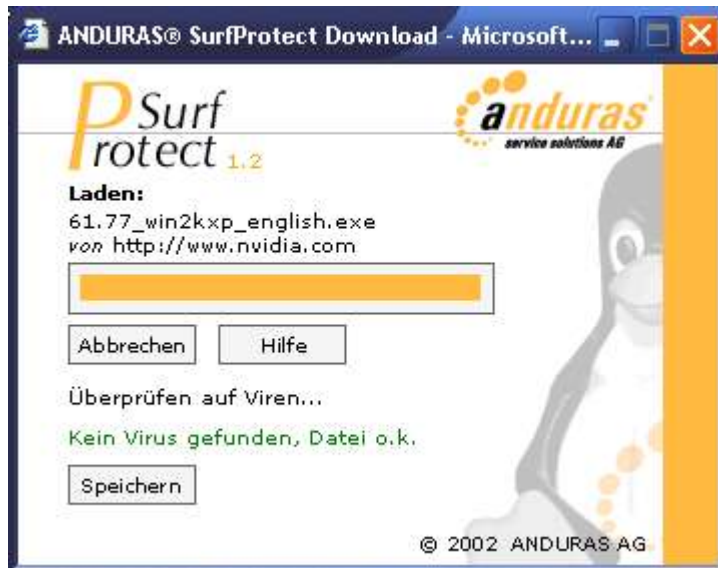




setzt man die Runlevels beider Programme gleich auf 3 und 5, damit sie auch beim nächsten Start automatisch gestartet werden. Bei den Clients und eventuell am Server muss man nun unter den Browsern Proxy aktivieren. Als IP-Adresse ist logischerweise die IP des Proxyserverns anzugeben und als Port 3128.



Beispielkonfiguration des Proxyserverns unter Windows XP und Internet Explorer.



Beispielscan von Surfprotect.



## 11. Nachtrag

Diese Machbarkeitsstudie ist von mir in alleiniger Erarbeitung entstanden. Natürlich lassen sich dadurch Fehler nicht vermeiden. Falls irgendwelche Fehler auftreten, diese mir bitte mitteilen. Man lernt schließlich gerne mal dazu.



## 12. Quellenangaben

Wichtige Quellen, die mir bei der Erstellung der Machbarkeitsstudie geholfen haben.

Aktuelle Ausgabe von Linux Intern für Virenschannerproxy

[http://www.gkainzbauer.de/computer/linux/linux\\_server/](http://www.gkainzbauer.de/computer/linux/linux_server/)

<http://www.afokken.de/linux/lxnames.htm>

[http://www.pl-forum.de/t\\_netzwerk/dhcpunddns.html](http://www.pl-forum.de/t_netzwerk/dhcpunddns.html)

[http://www.pl-berichte.de/work/server/samba\\_pdc.html](http://www.pl-berichte.de/work/server/samba_pdc.html)

## 13. Verfasser

Name:	Markus Roth
Geburtsdatum:	13.01.1983
Ort:	Göppingen
Ausbildungsberuf:	Fachinformatiker Fachrichtung Systemintegration
E-Mail:	ripuli2000@gmx.de